AMENDMENTS TO THE CLAIMS

1-17.   (Cancelled)

18.   (New) A distributed system for issuing printed objects, comprising:

a central control unit;

a plurality of local terminals that issue the printed objects, the local terminals located at different geographic locations, wherein each local terminal defines unequivocally a fingerprint;

a communication and control network through which the central control unit controls the local terminals;

a plurality of smart cards assigned to operators of the local terminals to activate and enable the local terminals to issue the printed objects, wherein each smart card includes a secret key; and

an initialization program that executes during an initialization stage following insertion of a given smart card in a corresponding given local terminal, wherein the initialization program is adapted to:

sign the fingerprint of the given local terminal with the secret key of the given smart card to generate a signed fingerprint,

send the signed fingerprint to the central control unit, and

establish a bi-unequivocable relationship between the given local terminal and the given smart card, whereby following the initialization stage, the given smart card is enabled to be used exclusively with the given local terminal, and the given local terminal is enabled for issuing

the printed objects exclusively after recognizing the given smart card.

19. (New) The system of claim 18, wherein the fingerprint comprises an "in the clear code" and an invisible or protected code.

20. (New) The system of claim 19, wherein the initialization program is adapted to execute following a customization step that associates the given smart card with a given account.

20. (New) The system of claim 19, wherein each local terminal includes a memory in which the "in the clear code" and the invisible or protected code are recorded prior to execution of the initialization program.

21. (New) The system of claim 19, wherein the initialization program is adapted to record the given smart card on the central control unit and enable the smart card for use with the given local terminal.

22. (New) The system of claim 19, wherein each smart card includes a data string that stores a personal identification code, and the initialization program is adapted to modify the data string on the given smart card to inhibit the personal identification code from being available to the operator of the given smart card.

23. (New) The system of claim 19, wherein the initialization program includes a double, asymmetrical key algorithm that signs the fingerprint of the given local terminal.

24. (New) The system of claim 18, wherein the initialization program comprises a protected, non-modifiable, machine program installed on each of the local terminals.

25. (New) The system of claim 18, wherein the initialization program is adapted to execute upon insertion of an uninitialized smart card into one of the local terminals.

26. (New) The system of claim 18, wherein the printed objects are selected from the group consisting of postage stamps, revenue stamps, stamped titles, and labels.

27. (New) The system of claim 18, wherein the given local terminal and the given smart card are adapted to perform local functions concerning issuance of the printed objects autonomously of the central control unit, and further wherein the given local terminal is adapted to transfer data relating to the local functions to the central control unit.

28. (New) A method for issuing printed objects, comprising:

      providing a central control unit;

      providing a plurality of local terminals that issue the printed objects, the local terminals located at different geographic locations, wherein each local terminal defines unequivocally a

fingerprint;

providing a communication and control network through which the central control unit controls the local terminals;

providing a plurality of smart cards assigned to operators of the local terminals to activate and enable the local terminals to issue the printed objects, wherein each smart card includes a secret key; and

initializing a given smart card for use with a corresponding given local terminal following insertion of the given smart card in the given local terminal, wherein the initializing step comprises:

signing the fingerprint of the given local terminal with the secret key of the given smart card to generate a signed fingerprint,

sending the signed fingerprint to the central control unit, and

establishing a bi-unequivocable relationship between the given local terminal and the given smart card, whereby following the initializing step, the given smart card is enabled to be used exclusively with the given local terminal, and the given local terminal is enabled for issuing the printed objects exclusively after recognizing the given smart card.

29. (New) The method of claim 28, further comprising obtaining the fingerprint by recording an "in the clear" code and an invisible code or protected code in a memory of the given local terminal.